Security Advisory | Volume 2018-12-02

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
[MS18-DEC] Microsoft .NET Framework Remote Code Injection Vulnerability - CVE-2018-8540	A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly, aka ".NET Framework Remote Code Injection Vulnerability." This affects Microsoft .NET Framework 3.5, 3.5.1, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2.	Version(s): Microsoft Dev Tools 4.62, 4.7.1, 4.7.2, 3.5SP1, 3.5.1, 3.5, 4.6, 4.5.2, 4.6.1, 4.7	Published - Dec 11, 2018 CVE-2018-8540 CVSS - 9.8 Vendor's Advisory - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8540 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8540
WordPress <5.0.1 Remote Unspecified Vulnerability - CVE-2018-20151	n WordPress before 4.9.9 and 5.x before 5.0.1, the user-activation page could be read by a search engine's web crawler if an unusual configuration were chosen. The search engine could then index and display a user's e-mail address and (rarely) the password that was generated by default.	Version(s) Wordpress Business Apps < 5.0.1	Published - Dec 14, 2018 CVE-2018-20151 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20151 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-20151
HAProxy Remote DoS Vulnerability - CVE-2018-20103	An issue was discovered in dns.c in HAProxy through 1.8.14. In the case of a compressed pointer, a crafted packet can trigger infinite recursion by making the pointer point to itself, or create a long chain of valid pointers resulting in stack exhaustion.	Version(s) HAProxy Business Apps <=1.8.14	Published - Dec 12, 2018 CVE-2018-20103 CVSS - 7.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20103 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-20103
SQLite <3.26.0 Remote Code Execution or DoS Vulnerability	SQLite, versions prior to 3.26, is prone to a remote code execution or a memory leak that might result in a denial-of-service.	Version(s): SQLite Business Apps < 3.2.6	Published - Dec 14, 2018 SBV-95293 CVSS - 9.8 Vendor's Advisory https://www.sqlite.org/releaselog/3_26_0.html https://thehackernews.com/2018/12/sqlite-vulnerability.html
Linux Kernel <4.19.9 Remote Unspecified Vulnerability - CVE-2018-20169	An issue was discovered in the Linux kernel before 4.19.9. The USB subsystem mishandles size checks during the reading of an extra descriptor, related to __usb_get_extra_descriptor in drivers/usb/core/usb.c.	Version(s): Linux Servers & Desktops < 4.19.9	Published - Dec 17, 2018 CVE-2018-20169 CVSS - 9.8 Vendor's Advisory -http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20169 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-20169
Google Kubernetes Remote Command Line Argument Injection Vulnerability - CVE-2018-1002101	In Kubernetes versions 1.9.0-1.9.9, 1.10.0-1.10.5, and 1.11.0-1.11.1, user input was handled insecurely while setting up volume mounts on Windows nodes, which could lead to command line argument injection.	Version(s): Google Business Apps 1.9.0- 1.9.9, 1.11.0 - 1.11.1, 1.10.0 - 1.10.5	Published - Dec 05, 2018 CVE-2018-1002101 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1002101 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1002101
WebSphere Application Server CSRF Vulnerability - CVE-2018-1926	BM WebSphere Application Server Admin Console is prone to cross-site request forgery vulnerability due to improper validation of user input. An attacker could send a malicious request to the server by enticing the victim to visit compromised URL.	Version(s):IBM Business Apps 7.0, 8.0, 9.0, 8.5	Published - Dec 10, 2018 CVE-2018-1926 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1926 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1926
Jenkins Remote Code Execution Vulnerability - CVE-2018-1000861	A code execution vulnerability exists in the Stapler web framework used by Jenkins 2.153 and earlier, LTS 2.138.3 and earlier in stapler/core/src/main/java/org/kohsuke/stapler/MetaClass.java that allows attackers to invoke some methods on Java objects by accessing crafted URLs that were not intended to be invoked this way.	Version(s): Pcloud Bees Dev Tools <= 2.138.3, 2.153	Published - Dec 10, 2018 CVE-2018-1000861 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000861 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1000861
Siemens TIM 1531 IRC Remote Privilege Escalation Vulnerability - CVE-2018-13816	TIM 1531 IRC, the communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7 with three RJ45, is missing proper authentication on port 102/tcp. A remote attacker could exploit this issue by sending packets to port 102/tcp of the affected device and perform arbitrary administrative operations.	Version(s):Siemens Other < 2.0	Published - Dec 11, 2018 CVE-2018-13816 CVSS - 10.0 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13816 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-13816